EXHIBIT 187

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DONNA CURLING, ET AL., **Plaintiffs,**	
v.	**DECLARATION OF** **J. ALEX HALDERMAN**
BRAD RAFFENSPERGER, ET AL., **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, I, J. ALEX HALDERMAN, declare under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. Curling Plaintiffs asked me to review and respond to two declarations submitted by James "Jim" Persinger, dated November 10 and December 13, 2022. In these declarations, Mr. Persinger attempts to downplay the damage he caused to evidence when he altered data on the Coffee County EMS Server—an act that violated the central tenet of digital forensics, which is that evidence should be collected and analyzed without changing the original source media. In his November

declaration, he claims that his actions altered only one file. His December declaration contradicts this and claims that only a different file was altered. In fact, Mr. Persinger's activities caused changes to *many hundreds of files*, among them files that contain evidence that is highly relevant to Plaintiffs' claims and to understanding the Coffee County breach.

3. Mr. Persinger is a "[redacted]."[1] He says he was retained by counsel for State Defendants in May 2021 to "[redacted]"[2] He also says that, more than a year later, State Defendants' counsel asked him to examine the Coffee County EMS Server and answer several questions related to the January 2021 security breach, including "[redacted]"[3] Those questions are relevant both to this lawsuit and to potential criminal prosecution of those responsible for the breach. Mr. Persinger says he executed a chain-of-custody document and took possession of the EMS Server from Center for Election Systems Director Michael Barnes on July 1, 2022, and that he photographed and forensically imaged the server on July 5, 2022.[4]

[1] Declaration of James "Jim" Persinger (Nov. 10, 2022) at ¶ 3 (hereinafter "Persinger First Decl.").

[2] Id. at ¶ 11.

[3] Id. at ¶ 12 and ¶ 14(b).

[4] Id. at ¶ 16, ¶ 17, and ¶ 22.

4. Standard forensic practice would be to perform all analysis using a *copy* of the data, such as the forensic image that Mr. Persinger says he created. However, Mr. Persinger makes the startling admission that just days after commencing work with the server, he changed the password *on the original server.*[5]

5. Mr. Persinger says that he changed the password "[redacted]"[6] This defies explanation. If a client needs to recover access to data on a server undergoing forensic examination, normal practice would be to provide the client a *copy* of the data, so as to preserve the integrity of the original evidence. Mr. Persinger easily could have made a copy of the hard drives for Mr. Barnes and then reset the password on that copy. It beggars belief that a "[redacted]" would deliberately alter the original data source, as Mr. Persinger admits he did.

6. Mr. Persinger states that at the time he received the Coffee County EMS Server and ImageCast Central Workstation, he "[redacted]"[7] This is not credible, for several reasons. With Mr. Persinger being a

[5] Id. at ¶ 23.
[6] Id. at ¶ 48.
[7] Id. at ¶ 16.

"[redacted]" and "[redacted]", he surely understood that preventing spoliation of evidence is a fundamental concern and a threshold issue for *any* work. Disclaiming his awareness in his declaration indicates he recognizes his error after the fact. Furthermore, this work request was from State Defendants' counsel, not from just any client, and it related to election technology, which is obviously consequential. The nature of the questions he was asked to address were probing for evidence that unauthorized activity and potentially criminal acts had taken place. The EMS Server is not only an essential piece of evidence for this matter but will also likely be an essential piece of evidence in any criminal prosecution arising from the Coffee County breach. Even if Mr. Persinger was completely ignorant of these circumstances, he certainly would have been put on notice that the EMS Server was to be "[redacted]" when he signed the "[redacted]" upon receiving it.[8]

7. Mr. Persinger's claim that he was "[redacted]" that the EMS Server was to be "[redacted]" is also inconsistent with actions he took before he changed the password. He says he photographed the machine and created a forensic image

[8] Id. at Exhibit C (emphasis in the original).

while employing a "[redacted]", a technology specifically designed to ensure that the original hard drive was not changed while he was imaging it.[9] These steps would be extraneous if one were not treating the server as "[redacted]."[10]

8. State Defendants have not explained why counsel for State Defendants would engage a "[redacted]" to reset a Windows login password, rather than simply utilizing the Secretary of State's information technology staff. Mr. Persinger states that "[redacted]"[11] Yet the server's hard drives were not encrypted, and there was no BIOS password set. In such a scenario, resetting a forgotten Windows password is a basic system administration task that can be accomplished by any competent information technology professional—and even by many home users—by following step-by-step instructions that are easily

[9] Id. at ¶ 21.

[10] Mr. Persinger claims that his policy is "[redacted]" (Id. at ¶ 29 (emphasis in the original)), but this is inconsistent with his stated actions. He says he took possession of the EMS Server and the ICC Workstation at the same time, on July 1, 2022, but he apparently did not image the ICC until months later, on September 15, 2022, after Plaintiffs scheduled their own expert to image it. Id. at ¶ 30.

[11] Id. at ¶ 14.

found online.[12] Even if the Secretary's in-house IT staff could not accomplish it, computer retailers such as Best Buy typically offer Windows password reset services for a nominal fee.

9. To confirm that the Windows login password for the Coffee County EMS Server could be easily reset, I carried out a widely documented password reset procedure on a *copy* of the server running in a virtual machine. Without making use of the original password, I changed the Windows password to a new password I selected, after which I was able to log in normally using the new password. The process took less than an hour and did not require the use of any third-party software or any computer security expertise. Since I performed the procedure using a *copy* of the data, it did not result in any changes to the original server or forensic images.

10. Mr. Persinger claims in his November declaration: "[redacted]"[13]

[12] See, for example, "Reset Windows 10 password without using third party tools", WINAERO (June 8, 2016). Available at https://winaero.com/reset-windows-10-password-without-using-third-party-tools/.

[13] Persinger First Decl. at ¶ 49.

11. The Court need not rely on Mr. Persinger's "[redacted]" to determine how many files were affected when Mr. Persinger changed the password. Mr. Persinger purports that he made a forensic image of the EMS Server "[redacted],"[14] before he changed the password. He later provided a copy of this image to Curling Plaintiffs' e-discovery specialist Robert Draper of Relevant Data Technologies. Mr. Draper also made his own image from the original EMS Server, on September 22, 2022. Mr. Draper performed the imaging process under Mr. Persinger's observation using specific forensic imaging software recommended by Mr. Persinger.[15]

12. These forensic images should represent complete snapshots of the data on the EMS Server on July 5, 2022, and September 22, 2022, respectively—i.e., from before and after Mr. Persinger changed the password. If there were no changes to the data on the server between those dates, then we would expect both images to be identical. I understand that the server remained in Mr. Persinger's possession for the entire period between when the images were created, and his November declaration

[14] Id. at ¶ 22. It is odd that Mr. Persinger is unable to precisely state on what date he imaged the EMS Server. The whole point of Exhibit E seems to be to show the metadata in a photograph he says he took during the imaging process, which indicates that it was taken on July 5, 2022, at 8:05 AM. Id. at Exhibit E. If Mr. Persinger is unsure himself whether this is a reliable record of when he imaged the system, how can Plaintiffs or the Court rely on it?

[15] Id. at ¶¶ 39-43.

states that, "[redacted]"[16] If this statement is true, then any differences between the two images are presumably attributable to Mr. Persinger changing the password. I directly compared the images to establish whether Mr. Persinger had altered any files.

13. The EMS Server contains two physical hard drives ("Drive 1" and "Drive 2") that normally function as a single logical hard drive. When the server was first deployed in 2019, it used what is called a "RAID-1" or "mirrored" storage configuration. This means both physical hard drives stored identical copies of each file, so that operation of the server could continue if either drive failed. There are several kinds of circumstances that can cause data on mirrored hard drives to differ, including accidental data corruption and malicious activity. Therefore, in performing my comparison, I ensured that I compared images created from the same physical hard drive.

[16] Id. at ¶ 51.

14. Specifically, I used the "[redacted]" image that Mr. Persinger describes creating in his November declaration, which has MD5 hash value [redacted]. Exhibit E from his November declaration indicates that this image was created from Drive 1, the hard drive with serial number [redacted], so I compared it to the "[redacted]" image that Mr. Draper created from the same Drive 1 with that same serial number. Mr. Draper's image has MD5 hash value [redacted].

15. I used standard software tools and techniques to locate differences between the two images and to determine whether any files or folders had been created, deleted, or altered. Working in an Ubuntu Linux environment, I mounted read-only copies of the server's "C: drive" from each image. I then used the command "diff -r -q" to list differences between the two copies. I wrote a simple Python script to annotate the results and convert them into a spreadsheet.

16. The table in Exhibit A shows the results of this comparison. Each row refers to an individual file by its name and specific location on the hard drive, which is known as the file's "path." The rows are colored according to the nature of each change (i.e., whether the file was created, deleted, appended to, or otherwise modified). Rather than differing in only one file, as they would if Mr. Persinger were correct, the images differ in 1,274 files or folders. While the server was in

Mr. Persinger's possession, 185 new files or folders were created on Drive 1, 349 were deleted, 21 were appended to, and 719 were otherwise modified.

17. I note that there are several reasonable ways to "count" changes to files on a hard drive, each of which will typically produce somewhat different results while supporting the same general conclusions. For example, one factor that complicates such an exercise is that certain files have what are effectively multiple names or paths. The methodology I used to prepare Exhibit A counts one change for each name or path by which a file can be referenced. If each change is counted once no matter how many names or paths reference the file (by invoking "diff" with the "--no-dereference" argument), then the images of Drive 1 differ in 501 files or folders: 58 were created, 99 deleted, 13 appended to, and 331 otherwise modified.

18. Among the many hundreds of files on the EMS Server that were altered by Mr. Persinger's activities are files that contain evidence of what occurred during the Coffee County breach. These include election project databases, Windows registry files (which store the system configuration and user settings), and numerous kinds of log files.

19. For example, Mr. Persinger's actions altered Windows event logs. These files document important activities related to the operation of the server and its security, and they are a primary source of information for experts when analyzing a

computer's prior activity. One of the Windows event logs, the System log, shows that the server was booted on July 6, 2022, at 8:07 AM. (I have added 75 days to account for the server's clock having been rolled back.[17]) The log indicates that this boot used a "one-time boot sequence," which is part of many widely documented procedures for resetting a Windows user password. Immediately after, the log records a successful login at 8:08 AM, a logout at 8:09 AM, and another login at 8:11 AM.[18] These log entries indicate that Mr. Persinger booted the EMS Server to change the password and then logged in twice, perhaps to test that the new password worked.

20. These actions caused changes to files throughout the hard drive. When a Windows system boots and when a user account logs in, the computer automatically performs many tasks in the background. Some tasks are configured to occur after every boot or login, while others may be configured to occur at a certain frequency

[17] Recall that someone rolled back the EMS Server's internal clock by 75 days on January 19, 2021, while Doug Logan and Jeff Lenberg were present in the Coffee County elections office. See Declaration of Kevin Skoglund (Dec. 5, 2022) at ¶¶ 105-107 (hereinafter "Skoglund Decl."); see also Nov. 22, 2022 Halderman Decl. at ¶ 18. There is no evidence that the server's clock was ever corrected, and Mr. Persinger's November declaration notes that the clock was still incorrect when he imaged the server. Persinger First Decl. at ¶ 20. The effect of this is that dates recorded by software running on the server must be corrected by adding 75 days.

[18] Mr. Persinger says he later sought to stop Plaintiffs' forensic expert Mr. Draper from booting the ICC Workstation, admonishing him that "[redacted]." Persinger First Decl. at ¶ 37 (emphasis added). Yet the System event log shows that Mr. Persinger himself powered on the EMS Server and worked with it without using a write blocker when he reset the Windows password.

(e.g., monthly) and so occur only if the computer has not been logged into for an extended period, as was the case with the EMS Server. For instance, automatic tasks may delete the oldest log files and create new ones, or they may write new data that overwrites areas of the hard drive that previously contained data from files that were deleted in the past.

21. As one example, Mr. Persinger's activities when he changed the password—and the automated tasks they initiated—added many new entries to three key Windows event logs. They added 77 events to the System log, 140 events to the Security log, and 128 events to the Application log. On the EMS Server, these logs are configured to have a fixed maximum size, so when new events are added, the oldest events are automatically deleted. Consequently, Mr. Persinger's activities caused the deletion of 89 events from the System log, 88 from the Security log, and 60 from the Application log.

22. It is likely that Mr. Persinger's activities also resulted in changes within the "unallocated space" of the hard drive, which often contains evidence about deleted files or data. Considering the unallocated space too would likely show even further changes caused by Mr. Persinger.

23. It would be costly and labor-intensive for Plaintiffs' experts to examine the many hundreds of files that have changed to determine how each individual change affected evidence relevant to this case.

24. Mr. Persinger's December declaration disputes the list of changes in my Exhibit A, which he refers to as "[redacted]."[19] He performed his own forensic image comparison using a convoluted methodology that involved proprietary software he created. I understand that State Defendants have refused to provide Plaintiffs a copy of this software to test.

25. Based on his comparison, Mr. Persinger concludes that "[redacted]"[20] Oddly, the one file Mr. Persinger's December declaration claims changed is a different file than the one file his November declaration claimed changed,[21] a contradiction that he does not acknowledge or explain.

26. One problem with Mr. Persinger's analysis is that it neglects the fact that totally different files contained in different folders sometimes have the same name.

[19] This list was exchanged with the Court and counsel at the November 15, 2022 Status Conference. See Dkt. 1544 at 21:20-22:4.

[20] Declaration of James "Jim" Persinger (Dec. 13, 2022) at ¶ 46 (hereinafter "Persinger Second Decl.").

[21] Compare with Persinger First Decl. at ¶ 49.

This is why the list of changes I produced shows each file's specific location. Mr. Persinger ignored this information and compared files from anywhere on the server that happened to have the same name as the ones from my table. Of the 465 files or folders that he compared, 343 do not appear on my list at all; they are entirely separate files or folders that nobody claims were altered. Therefore, his "[redacted]"[22] of "[redacted]"[23] does not measure any relevant quantity.

27. More significantly, in every case where Mr. Persinger and I *do* disagree about whether a file has been altered, his results are erroneous. One need only examine a few of these files to see that his findings are flawed.

28. One example is "[redacted]" The screenshot below shows a freely available software application that is used to visually compare two versions of a file. The left side of the screen shows the file from the pre-password-change image I examined, and the right side shows the same file from the post-password-change image I examined. I have scrolled both sides to the bottom to show the ends of the files. They are different: the lines highlighted in green exist only in the post-password-change

[22] Persinger Second Decl. ¶ 51.
[23] Id.

version. They are log entries timestamped April 22, 2022, which, adjusting for the server's clock, is July 6—the day Mr. Persinger changed the password.

[redacted]

29. Another file that Mr. Persinger erroneous concludes was not altered is "[redacted]." The screenshot below uses the same format as the previous one, showing the pre-password-change version of this file on the left and the post-password-change version of the same file on the right. Once again, the highlighted lines exist only in the image from after Mr. Persinger changed the password, and they are timestamped on the day he changed the password.

[redacted]

30. A third file that Mr. Persinger mistakenly concludes was not altered is "[redacted]." The screenshot below shows, yet again, that the pre-password-change and post-password-change versions of this file differ, because log entries were added on the day Mr. Persinger changed the password.

[redacted]

31. These files have demonstrably been altered, despite Mr. Persinger's analysis to the contrary, and, given the timestamps, the only plausible explanation for the changes is that the files were altered due to his activities around the time he changed the password. Moreover, Mr. Persinger's error extends well beyond the three examples shown above.[24] In response to his analysis, I reconfirmed each of the differences listed in my Exhibit A by comparing the hashes values of the individual

[24] I selected the three files shown above because the changes in them are relatively easy to interpret by inspection. The vast majority of the files that were altered have more complicated differences, such as changes to non-human-readable data, and, in most cases, data has been at least partially overwritten or deleted, rather than merely appended to as in these examples.

files, and in *every instance* where Mr. Persinger's December declaration disputes that a file listed in my table was modified, he is wrong.

32. Although Mr. Persinger's description of his comparison methodology is vague, it appears likely that the main reason his results differ so dramatically from mine is that he compared the *wrong hard drive*.

33. As I noted above (see supra at ¶ 13), the EMS Server has two physical hard drives ("Drive 1" and "Drive 2"), which were originally "mirrored" such that both contained identical copies of every file.

34. Mr. Draper imaged both Drive 1 and Drive 2. Mr. Persinger's November declaration admonishes him for having imaged both drives,[25] implying that Mr. Persinger believed both drives would have the same data. However, Mr. Draper was following good practice; a careful forensic analysis would not take for granted that the drives were identical, and, in this instance, they are not.

35. Examining Mr. Draper's images of Drive 1 and Drive 2 together shows that the physical hard drives appear to have become *unmirrored* at some point between the date when Mr. Persinger took possession of the server and when he changed the password. After the drives became unmirrored, the EMS Server used

[25] Persinger First Decl. at ¶ 43.

Drive 1 exclusively, and the data on Drive 1 and Drive 2 diverged. Consequently, an accurate view of the changes Mr. Persinger caused when he reset the password requires comparing images of Drive 1.

36. The serial number recorded in the log file Mr. Persinger provided with his pre-password-change image indicates that the image was created from Drive 1. Comparing Mr. Persinger's pre-password-change image of Drive 1 to Mr. Draper's post-password-change image of Drive 1 reveals the large set of modified files I have reported. However, comparing Mr. Persinger's pre-password-change image of Drive 1 to Mr. Draper's post-password-change image of *Drive 2* yields differences in only approximately five files, including the "[redacted]" that Mr. Persinger's December declaration finds to have changed. This is consistent with Drive 2 becoming unmirrored from Drive 1 before the password change and the hundreds of other resulting changes.

37. From this I conclude that Mr. Persinger erroneously based his analysis on data from Drive 2. Mr. Persinger's analysis, therefore, does not accurately reflect how many files he altered when he changed the password.

38. The fact that the server's formerly mirrored hard drives now contain significantly different data raises further questions about its forensic integrity. When and why did the drives become "[redacted]"? If Mr. Persinger was aware that the

drives are no longer mirrored, why he did not remark on it in either of his declarations, despite its immediate relevance?

39. Drives can be unmirrored automatically if the system detects that a drive has failed due to wear or damage, or an operator can unmirror them by changing the system's settings (typically through the BIOS configuration) or by physically disconnecting a drive. In this instance, I have insufficient information to determine the cause, but the data does indicate a timeframe. I compared the Windows System event logs from Mr. Draper's images of Drive 1 and Drive 2. Both logs appear to be the same through the evening of July 1, 2022 (adjusted for the server's clock), implying that the drives were still mirrored on this date. After July 1, the log from Drive 2 stops and the log from Drive 1 records further entries associated with Mr. Persinger changing the password. Since Mr. Persinger took possession of the server on July 1, this implies that the drives became unmirrored sometime between the day he received it and when he reset the password.

40. Throughout his declarations, Mr. Persinger expresses the view that Plaintiffs can simply verify the hash value of the pre-password-change image he provided and then rely on that image as if it were the original, unmodified hard drive. "[redacted]," he says, "[redacted]

[redacted] ."[26] Yet this misstates the evidentiary value of hashes. For the purposes at issue, a hash value can be thought of as a compact way of representing the content of a data source, such as a file or forensic image. If two images have the same hash value, we can be confident that the data they contain is identical. Here, Mr. Persinger provided both the image file and its hash value, and Plaintiffs have only his say-so that either the image or the hash value represents the unmodified state of the server. Verifying the hash value says nothing about whether the image Mr. Persinger provided matches what was *ever* on the EMS Server, let alone that it represents an accurate copy of server's contents when he received it.

41. It is likely that neither Mr. Persinger's pre-password-change image nor the post-password-change image *of either hard drive* reflects the server's unmodified contents when Mr. Persinger received it from the Secretary of State's Office. Mr. Persinger himself, in his December declaration, found that there are files on the server with metadata indicating that they were created or modified at approximately 7:30 PM on April 17, 2022.[27] When accurately corrected for the server's clock,[28] this

[26] Persinger First Decl. at ¶ 21.

[27] Persinger Second Decl. at ¶ 18 and Exhibits B and C thereto, among others.

[28] Note that Exhibit L attached to Mr. Persinger's second declaration appears to give a misleading result for this date correction. It is a screenshot from a date calculator website showing that the number of days from April 17 to *June 30* is 75. However, a box is checked

is the evening of July 1, 2022—the day Mr. Persinger took possession of the server and signed a chain of custody log to that effect. This indicates that changes occurred to the original EMS Server either shortly after the server entered Mr. Persinger's possession or else immediately before it was transferred to him.

42. The System event log from Mr. Persinger's July 5, 2022, image shows that the server was not booted at all for almost three months prior to July 1, 2022. Then, that evening, it was booted and powered off twice in the span of a few minutes at around the same time the files changed. One possible explanation for the changes that would be consistent with these log entries is that Mr. Persinger booted the system without a write-blocker in place, just as he later did when he changed the password.

43. Comparing images of Drive 1 and Drive 2 shows that identical changes dated July 1, 2022, are present on both hard drives. This indicates that the drives were still mirrored when the changes occurred. Thus, they are present in the image Mr. Persinger created of Drive 1 on July 5 as well as in Mr. Draper's later image of Drive 2. (Some of the changes are also present on Mr. Draper's image of Drive 1, but others were overwritten by subsequent changes when Mr. Persinger reset the

labeled "[redacted]" I tested the same site, and this box causes it to count days inclusively, i.e., including the both the first and the last date in the 75. However, to accurately correct the server's clock, one must instead calculate the *75th day* from April 17, which is July 1.

password.) In both images, at least 130 files have modification dates indicating that they were changed on the evening of July 1, 2022, including many of the same log files, election database files, and Windows registry files that were also affected when Mr. Persinger changed the password. Since these changes affected both drives, Plaintiffs cannot rely on the image of either drive as if it were the original, unmodified hard drive.

44. The changes that occurred to both drives on July 1, 2022, are *in addition* to the changes that occurred to Drive 1 when Mr. Persinger reset the password on July 6, 2022, that I list in Exhibit A. I generated those results by comparing Mr. Persinger's pre-password-change image to a later image of the same drive, and they do not rely on file modification dates. Because my comparison used the pre-password-change image as the baseline, it would not reveal changes caused by Mr. Persinger between when he took possession of the server on July 1, 2022, and when he purportedly created the pre-password-change image on July 5, 2022.

45. Mr. Persinger's declarations contain other mistakes and inconsistencies in addition to those that I have already noted. For instance, in his December declaration, he disputes "[redacted]", which he

says is July 5, 2022.[29] Citing a log that was generated when he created his initial image, which is dated April 21 due to the server's incorrect clock, he states: “[redacted].”[30]

46. There are several problems with this argument. First, it is circular, as Mr. Persinger presupposes that no changes occurred after he imaged it. Even then, if we were to consider only changes prior to Mr. Persinger's imaging process, the last date that files could have changed would be the day he imaged the server, and it is logically impossible that he imaged it “[redacted]” to taking possession of it. The reason for this apparent paradox is that Mr. Persinger's math is wrong: 75 days after April 21 is not June 30 but July 5—the date his November declaration states he imaged the server. The Exhibit L he cites in arriving at “[redacted]” is a screenshot of a date calculator website, but it shows that there are 75 days (counting inclusively) between June 30 and *April 17*, not April 21. These errors create further doubt about the reliability of Mr. Persinger's work.

[29] Persinger Second Decl. at ¶ 17.

[30] Id. at ¶ 18 (emphasis in the original).

47. Mr. Persinger caused extensive changes to the original EMS Server by resetting the password while following a practice that he himself calls "[redacted][31] He now attempts to argue that Plaintiffs should rely on an image of the server he created, yet there is evidence that Mr. Persinger caused other extensive changes to both of the server's mirrored hard drives before he created that image. The image, therefore, does not represent the unmodified state of the server as he received it. These inexplicable deviations from normal forensic practice leave Plaintiffs with no copy of the unmodified contents of the EMS Server prior to Mr. Persinger's changes.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 7th day of January, 2023 at Melbourne, Australia.

J. ALEX HALDERMAN

[31] Persinger First Decl. at ¶ 37.